(19)日本国特許庁(JP)　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開２００２－２５９６０６
（Ｐ２００２－２５９６０６Ａ）
(43)公開日　平成14年9月13日(2002.9.13)

(51)Int.Cl.⁷		識別記号	FI			テーマコード(参考)
Ｇ０６Ｆ	17/60	１４２	Ｇ０６Ｆ	17/60	１４２	5B076
		３０２			３０２　Ｅ	
		３４０			３４０	
		５０４			５０４	
	1/00			9/06	６６０　Ｃ	

審査請求　未請求　請求項の数１８　ＯＬ　（全１３頁）

(21)出願番号　特願2001-55976(P2001-55976)

(22)出願日　平成13年2月28日(2001.2.28)

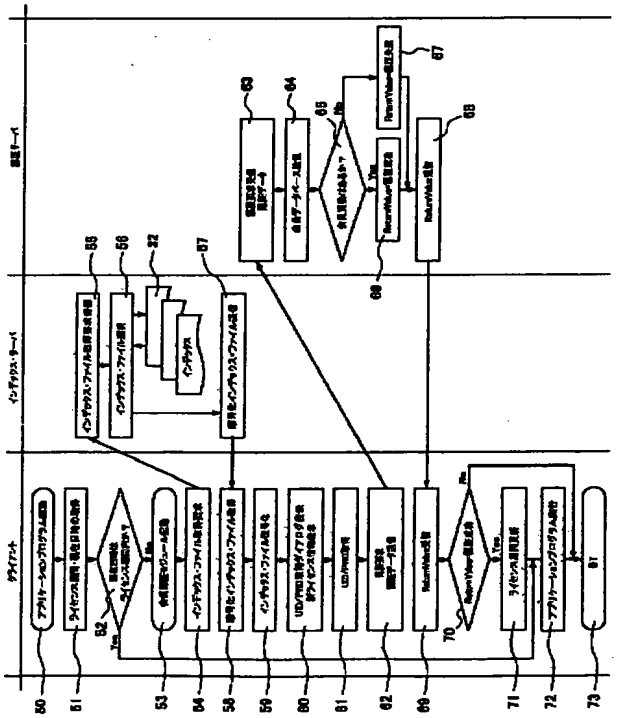
(71)出願人　390009531
インターナショナル・ビジネス・マシーンズ・コーポレーション
INTERNATIONAL BUSINESS MASCHINES CORPORATION
アメリカ合衆国10504、ニューヨーク州　アーモンク　ニュー　オーチャード　ロード

(74)復代理人　100112520
弁理士　林　茂則　（外2名）

最終頁に続く

(54)【発明の名称】プログラム使用許諾期間の更新方法、プログラムの使用許諾方法、情報処理システムおよびプログラム

(57)【要約】
【課題】　プログラム使用許諾（ライセンス）期間の更新を自動的に行う。
【解決手段】　現在日時がプログラムの使用許諾期間内であるかを判断し（ステップ５２）、インデックス・サーバにインデックス・ファイルの送信要求を発し（ステップ５４）、インデックス・サーバからインデックス・ファイルを受信し（ステップ５８）、インデックス・ファイルに含まれる認証サーバのアドレスに、認証要求を発し（ステップ６２）、認証サーバから認証情報を受信し（ステップ６９）、認証成功の場合にはプログラムの使用許諾期間を更新し（ステップ７１）。プログラムを実行する（ステップ７２）。



【特許請求の範囲】

【請求項１】　現在日時がプログラムの使用許諾期間内であるかを判断する第１判断ステップと、
前記第１判断ステップの前記判断が偽の場合、インデックス・サーバに対し、インデックス・ファイルの送信要求を発するステップと、
前記インデックス・サーバからインデックス・ファイルを受信するステップと、
前記インデックス・ファイルに含まれる認証サーバのアドレスに、認証要求を発するステップと、
前記認証サーバから認証情報を受信するステップと、
前記認証情報に認証成功の情報が含まれるかを判断する第２判断ステップと、
前記第２判断ステップの前記判断が真の場合、前記プログラムの使用許諾期間を更新するステップと、
を含むプログラム使用許諾期間の更新方法。

【請求項２】　前記第１判断ステップは、前記プログラムの起動を契機として実行され、
前記使用許諾期間の更新の後に前記プログラムの実行が可能になる請求項１記載の方法。

【請求項３】　前記インデックス・ファイルに含まれる前記認証サーバのアドレス情報が暗号化されており、
前記暗号化された前記認証サーバのアドレス情報を復号化するステップをさらに有する請求項１記載の方法。

【請求項４】　前記認証要求には、前記プログラムの使用が許諾されているグループに属すか否かを判断するためのユーザ識別情報を含み、
前記認証サーバは、前記グループを管轄する者が管理するものである請求項１記載の方法。

【請求項５】　前記認証要求を発する前に、前記ユーザ識別情報とパスワードとを入力するよう要求する画面を表示するステップをさらに有する請求項４記載の方法。

【請求項６】　前記インデックス・ファイルには前記プログラムの使用許諾条件に関する情報が含まれており、
前記画面には、前記ユーザ識別情報とパスワードの入力要求に加えて前記プログラムの使用許諾条件に関する情報を表示する請求項５記載の方法。

【請求項７】　ユーザからの要求を受取るステップと、
前記要求の受信を契機として、前記ユーザが使用するプログラムの使用許諾に関する認証を与えるサーバのアドレス情報を含むインデックス・ファイルを生成または選択するステップと、
前記インデックス・ファイルを前記要求を発したユーザに送信するステップと、
を有するプログラムの使用許諾方法。

【請求項８】　前記インデックス・ファイルに含まれる前記アドレス情報の部分は暗号化される請求項７記載の方法。

【請求項９】　現在日時がプログラムの使用許諾期間内であるかを判断する第１判断手段と、
前記第１判断手段の前記判断が偽の場合、インデックス・サーバに対し、インデックス・ファイルの送信要求を発する手段と、
前記インデックス・サーバからインデックス・ファイルを受信する手段と、
前記インデックス・ファイルに含まれる認証サーバのアドレスに、認証要求を発する手段と、
前記認証サーバから認証情報を受信する手段と、
前記認証情報に認証成功の情報が含まれるかを判断する第２判断手段と、
前記第２判断手段の前記判断が真の場合、前記プログラムの使用許諾期間を更新する手段と、
を含む情報処理システム。

【請求項１０】　前記第１判断手段は、前記プログラムの起動を契機として実行され、
前記使用許諾期間の更新の後に前記プログラムが実行可能になる請求項９記載のシステム。

【請求項１１】　前記インデックス・ファイルに含まれる前記認証サーバのアドレス情報が暗号化されており、
前記暗号化された前記認証サーバのアドレス情報を復号化する手段をさらに有する請求項９記載のシステム。

【請求項１２】　前記認証要求には、前記プログラムの使用が許諾されているグループに属すか否かを判断するためのユーザ識別情報を含み、
前記認証サーバは、前記グループを管轄する者が管理するものである請求項９記載のシステム。

【請求項１３】　前記ユーザ識別情報とパスワードとを入力するよう要求する画面を表示する手段をさらに有する請求項１２記載のシステム。

【請求項１４】　前記インデックス・ファイルには前記プログラムの使用許諾条件に関する情報が含まれており、
前記画面には、前記ユーザ識別情報とパスワードの入力要求に加えて前記プログラムの使用許諾条件に関する情報を表示する請求項１３記載のシステム。

【請求項１５】　ユーザからの要求を受取る手段と、
前記要求の受信を契機として、前記ユーザが使用するプログラムの使用許諾に関する認証を与えるサーバのアドレス情報を含むインデックス・ファイルを生成または選択する手段と、
前記インデックス・ファイルを前記要求を発したユーザに送信する手段と、を有する情報処理システム。

【請求項１６】　前記インデックス・ファイルに含まれる前記アドレス情報の部分を暗号化する手段をさらに有する請求項１５記載のシステム。

【請求項１７】　現在日時がプログラムの使用許諾期間内であるかを判断する第１判断機能と、
前記第１判断機能の前記判断が偽の場合、インデックス・サーバに対し、インデックス・ファイルの送信要求を発する機能と、

前記インデックス・サーバからインデックス・ファイルを受信する機能と、
前記インデックス・ファイルに含まれる認証サーバのアドレスに、認証要求を発する機能と、
前記認証サーバから認証情報を受信する機能と、
前記認証情報に認証成功の情報が含まれるかを判断する第２判断機能と、
前記第２判断機能の前記判断が真の場合、前記プログラムの使用許諾期間を更新する機能と、
をコンピュータに実現させるためのプログラム。
【請求項１８】　ユーザからの要求を受取る機能と、
前記要求の受信を契機として、前記ユーザが使用するプログラムの使用許諾に関する認証を与えるサーバのアドレス情報を含むインデックス・ファイルを生成または選択する機能と、
前記インデックス・ファイルを前記要求を発したユーザに送信する機能と、
をコンピュータに実現させるためのプログラム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、プログラムの使用許諾期間（ライセンス期間）の更新方法、情報処理システムおよびプログラムに関する。特に、ライセンス期間が満了した場合のライセンス更新を簡略化し、ユーザに煩雑な手続を強いることのないライセンス更新に適用して有効な技術に関する。
【０００２】
【従来の技術】コンピュータ・プログラムは著作権で保護されるため、著作権フリーないわゆるフリーウェアを除き、ライセンス方式によってその使用が許諾されるのが一般的である。一般にユーザはプログラムを購入する際に個人的な使用が許諾され、特に使用期限が設けられない場合もある。
【０００３】しかし、たとえば、いわゆるシェアウェアや試用プログラムのように、特定の期間無料または廉価で試用させ、その後さらに使用を希望するユーザにさらに使用許諾（ライセンス）を与える場合もある。この使用許諾に使用期限（ライセンス期間）を設ける場合も多い。
【０００４】ライセンス期間が設けられるプログラムには、ライセンスキーあるいはプロダクトキーが与えられ、正当なキーと正当な期間情報が与えられてプログラムの全ての機能が実行されるようになっているのが一般的である。すなわち、ユーザはプログラムの使用許諾元から発行された正当なキー情報を入力し、かつ、正当な期間（ライセンス期間）内での使用でなければプログラムを利用することができない。
【０００５】そこで、ライセンス期間が経過した場合、さらにプログラムの使用を希望するときには、ユーザは使用許諾元（プログラム提供者）から新たなライセンスキーを入手する必要がある。新たなライセンスキーの入手は、一般に、メール等によるユーザからのライセンス更新申請、プログラム提供者による更新申請の認証、プログラム提供者による更新キーの発行送付、ユーザによる更新キーの適用、というステップを経る。
【０００６】
【発明が解決しようとする課題】しかしながら、前記した新たなライセンスキー（更新キー）の申請・発行・取得の手続はユーザおよびプログラム提供者の双方にとって煩雑である。すなわち、ユーザはライセンス期間内にはほとんど意識することがなかった更新手続を行う必要があり、プログラム提供者にとってはユーザからの申請に個別に対応しなければならない。さらにユーザは新たな更新キーを適用しなければならない。このような事務手続を簡略化するためにライセンス期間を相当に長くする方策も考え得るが、ライセンス期間を短くして有効に対価を回収したい場合にはその要求に反する。
【０００７】あるいは特定の会（クラブ）を結成し、この会員向けに特定のプログラムを包括的に使用許諾するような場合には、プログラムごとにライセンス更新の申請を受け付けていてはその認証事務手続が膨大になり効率化が強く要請される。
【０００８】本発明の目的は、プログラム使用許諾（ライセンス）期間の更新認証事務を効率化することにある。また、本発明の目的は、ライセンス期間を自動的に更新できる技術を提供することにある。また、本発明の目的は、ユーザおよびプログラム提供者の双方に利便性の高いライセンス更新システムを提供することにある。また、本発明の目的は、システムの利便性のみならず、セキュリティおよびフレキシビリティに優れたライセンス更新システムおよび方法を提供することにある。
【０００９】
【課題を解決するための手段】本願の発明の概略を説明すれば、以下の通りである。すなわち、本発明のプログラム使用許諾期間の更新方法は、現在日時がプログラムの使用許諾期間内であるかを判断する第１判断ステップと、第１判断ステップの判断が偽の場合、インデックス・サーバに対し、インデックス・ファイルの送信要求を発するステップと、インデックス・サーバからインデックス・ファイルを受信するステップと、インデックス・ファイルに含まれる認証サーバのアドレスに、認証要求を発するステップと、認証サーバから認証情報を受信するステップと、認証情報に認証成功の情報が含まれるかを判断する第２判断ステップと、第２判断ステップの判断が真の場合、プログラムの使用許諾期間を更新するステップと、を含む。
【００１０】なお、プログラムの起動を契機に前記第１ステップが実行され、使用許諾期間の更新の後にプログラムが実行可能となるようにしても良い。また、アドレス情報が暗号化され、この暗号化されたアドレス情報を

復号化するステップを有しても良い。また、認証要求には、プログラムの使用が許諾されているグループに属すか否かを判断するためのユーザ識別情報を含み、認証サーバは、このグループを管轄する者が管理するものであってもよい。さらに、認証要求を発する前に、ユーザ識別情報とパスワードとを入力するよう要求する画面を表示し、この画面にはプログラムの使用許諾条件に関する情報を表示しても良い。

【００１１】本発明によれば、ライセンス期間の満了を自動的に判断して、プログラム提供者（認証サーバ）に自動的に認証要求を発する。認証結果は認証サーバからユーザに返送され、ライセンス期間が自動的に更新される。このためユーザは更新キーの発行を申請することなく、簡便にプログラムのライセンスを再度得ることができる。一方、プログラム提供者は、ユーザからの更新申請が定式化されて送付されるので認証の自動化が可能であり、また、ユーザの更新要求はインデックス・サーバを参照して行われるので認証サーバの変更を容易に行うことができる。すなわち、認証サーバを変更しても、ユーザに対するアドレス送付の必要はなく、インデックス・サーバのインデックス・ファイルを更新するのみで認証サーバのアドレスを変更できる。また、ユーザはインデックス・サーバから認証サーバのアドレス情報を取得するので、認証サーバのアドレスを公開する必要がなく認証サーバのセキュリティを向上できる。また、送付されるアドレス情報は暗号化できるのでさらにセキュリティを向上できる。

【００１２】本発明は、たとえばユーザを会員とする組織にプログラムを許諾する場合に好適なものである。プログラム提供者はユーザの識別情報を会員番号として管理し、会員である限りプログラム使用のライセンスを与える場合などに適用できる。この場合、ユーザはライセンス期間の自動更新に際して会員であることの証明であるユーザ識別情報（会員番号）とパスワードを認証サーバの送信する。本発明では、このような会員番号（識別情報）の入力画面を備える。認証サーバは会員データベースを参照して有効な会員であれば認証を与える。

【００１３】また、本発明は、ユーザからの要求を受取るステップと、要求の受信を契機として、ユーザが使用するプログラムの使用許諾に関する認証を与えるサーバのアドレス情報を含むインデックス・ファイルを生成または選択するステップと、インデックス・ファイルを要求を発したユーザに送信するステップと、を有するプログラムの使用許諾方法である。なお、インデックス・ファイルに含まれるアドレス情報の部分は暗号化することができる。このような方法によりユーザはインデックス・ファイルを取得できる。

【００１４】なお、本発明の方法は、システムあるいはプログラムとして把握することも可能である。

【００１５】【発明の実施の形態】以下、本発明の実施の形態を図面に基づいて詳細に説明する。ただし、本発明は多くの異なる態様で実施することが可能であり、本実施の形態の記載内容に限定して解釈すべきではない。なお、実施の形態の全体を通して同じ要素には同じ番号を付するものとする。

【００１６】以下の実施の形態では、主に方法またはシステムについて説明するが、当業者であれば明らかなとおり、本発明はコンピュータで使用可能なプログラムとしても実施できる。したがって、本発明は、ハードウェアとしての実施形態、ソフトウェアとしての実施形態またはソフトウェアとハードウェアとの組合せの実施形態をとることができる。プログラムは、ハードディスク、ＣＤ－ＲＯＭ、光記憶装置または磁気記憶装置等の任意のコンピュータ可読媒体に記録できる。

【００１７】また以下の実施の形態では、クライアントのシステムおよびサーバのシステムとして、一般的なコンピュータシステムを用いることができる。実施の形態で用いることができるコンピュータシステムは、中央演算処理装置（ＣＰＵ）、主記憶装置（メインメモリ：ＲＡＭ）、不揮発性記憶装置（ＲＯＭ）、コプロセッサ、画像アクセラレータ、キャッシュメモリ、入出力制御装置（Ｉ／Ｏ）等、一般的なコンピュータシステムに備えられるハードウェア資源を備える。また、ハードディスク装置等の外部記憶装置、インターネット等のネットワークに接続可能な通信手段を備えることができる。コンピュータシステムには、パーソナルコンピュータ、ワークステーション、メインフレームコンピュータ等各種のコンピュータが含まれる。

【００１８】図１は、本発明の一実施の形態であるライセンス期間の更新方法に適用できるシステムの一例を示した概念図である。本実施の形態のシステムは、インターネット１に、クライアントのコンピュータシステム２、インデックス・サーバ３、認証サーバ４が接続されている。

【００１９】インターネット１は、良く知られているように、ＩＰ（Internet Protocol）に従って通信が行われる世界的に開かれたネットワークの一形態である。ここではインターネットを例示するが、他のネットワーク形態を利用することも可能である。たとえば専用電話線により接続されたネットワークあるいはＣＡＴＶ等のケーブルネットワークでもよい。インターネットの概念には、特定の者にのみ利用が制限されるイントラネットも含む。

【００２０】クライアントのコンピュータシステム２（以下単にクライアント２という）は、プログラム提供者等によって使用許諾（ライセンス）が与えられるプログラムを使用するユーザのコンピュータシステムである。プログラムにはアプリケーション・プログラムが例示できる。以下の説明では、クライアント２として一般

的なコンピュータシステムを例示して説明するが、携帯電話６、携帯情報端末（ＰＤＡ：Personal Digital Assistants）７等がクライアント２として機能してもよい。また、図１では単一のクライアント２として表現しているが、クライアント２が多数存在することは言うまでもない。

【００２１】インデックス・サーバ３は、ユーザの要求に応じて、認証サーバ４のＵＲＬ（uniform resource locator）を含むインデックス・ファイルをユーザに送信する機能を持つ。認証サーバ４は、ユーザからのライセンス期間更新要求に対して認証を与える機能を持つ。インデックス・サーバ３および認証サーバ４には、前記したとおり一般的なコンピュータシステムが利用できる。また、図１では各々単一のインデックス・サーバ３および認証サーバ４として表現しているが、複数のインデックス・サーバ３および認証サーバ４が存在してもよい。

【００２２】図２は、本実施の形態のライセンス期間更新の概要について時系列に示した図である。時刻ｔ０でユーザがアプリケーション・プログラムをダウンロードする場合を考える（ステップ１０）。なお、ユーザはこの時点でプログラム提供者の管理するグループ（会）の会員であるとする。ダウンロードの時からアプリケーション・プログラムのライセンス期間が開始し、ライセンスは時刻ｔ０～ｔ２の間で有効であるとする。この期間（ｔ０～ｔ２）は、プログラムをインストールする際に同意したライセンス期間となる。時刻ｔ１でユーザがアプリケーション・プログラムを起動した時、ライセンスは有効であるためアプリケーション・プログラムが実行できる（ステップ１１）。

【００２３】一方、ライセンス期間が時刻ｔ２で満了した後の時刻ｔ３にユーザがアプリケーション・プログラムを実行しようとすると、従来であればライセンスが有効ではないためプログラムの実行はできない。しかし、本実施の形態では、アプリケーション・プログラムの起動を契機としてユーザの認証を自動的に行い、ライセンス期間を自動的に更新する（ステップ１２）。この場合、ユーザの会員資格は依然有効であるため認証が成功しライセンス期間が時刻ｔ４まで更新されてアプリケーション・プログラムが実行可能になる。なお、この更新の際のライセンス期間（ｔ３～ｔ４）は、前記プログラムをインストールする際のライセンス期間（ｔ０～ｔ２）と相違しても良い。更新されたライセンス期間は、更新の際のライセンス（契約）に従う。たとえば試用目的に廉価でプログラムを頒布し、その後正式に対価を支払ってプログラムを利用するような場合、試用のライセンス期間（プログラムダウンロードの際のライセンス期間）を１ヶ月程度と短くし、正式契約（更新）の際のライセンス期間を１年程度に長くできる。

【００２４】時刻ｔ５でユーザがグループから脱会した場合（ステップ１３）、ユーザが会員資格がない期間の時刻ｔ６でアプリケーション・プログラムを起動すると、本実施の形態のシステムは前記同様に認証確認を行うが会員資格が無効なので認証に失敗し、ライセンス期間は更新されず、結果としてアプリケーション・プログラムの実行はできない（ステップ１４）。

【００２５】しかしながら、ユーザが時刻ｔ７で再度グループに入会した場合（ステップ１５）、それ以降の時刻ｔ８にユーザがアプリケーション・プログラムを実行すると、前記ステップ１２の場合と同様にライセンスが有効になり、アプリケーション・プログラムが実行できるようになる（ステップ１６）。すなわち、本実施の形態のシステムは会員資格が有効である限りユーザに認証が与えられてアプリケーション・プログラムが利用できるようになるシステムである。

【００２６】図３は、クライアント２、インデックス・サーバ３、認証サーバ４の構成の一例を示したブロック図である。

【００２７】クライアント２には、アプリケーション・プログラム２０を有し、アプリケーション・プログラム２０には、ライセンス期間チェックモジュール２１、会員認証モジュール２２、アプリケーション実行モジュール２３を有する。また、クライアント２には時計２４を有する。

【００２８】アプリケーション・プログラム２０は、プログラム提供者から提供されるプログラムである。なお、ここではアプリケーション・プログラムを例示するが、プログラム提供者から提供されるプログラムはアプリケーション・プログラムには限られない。たとえば特定のシステムで稼動するシステムプログラム、特定のアプリケーションで利用可能なマクロプログラム等であってもよい。

【００２９】ライセンス期間チェックモジュール２１は、アプリケーション・プログラムの起動に際して起動され、現在時刻がライセンス期間内にあるかを判断する機能を持つ。現在時刻は時計２４から取得できる。なお、ライセンス期間の情報はクライアント２のシステムの何れかの記憶領域に記録されるほか、適当な通信回線で接続されている他のシステムに記録されても良い。この場合、多数のユーザのライセンス期間を一元的に管理できる。またこの場合、ライセンス期間チェックモジュール２１は、このような通信機能をも有し、適切な情報を取得する手段を有する。

【００３０】会員認証モジュール２２は、インデックス・サーバ接続手段２２１、インデックス・ファイル取得手段２２２、取得情報デコーダ２２３、ＵＩＤ／ＰＷＤ取得・新ライセンス表示ダイアログ２２４、認証サーバ接続手段２２５、認証結果取得手段２２６、認証結果チェック手段２２７を有する。

【００３１】インデックス・サーバ接続手段２２１は、インデックス・サーバ３に対しインデックス・ファイル

を取得するよう要求を発する。なお、この要求には適切なインデックス・ファイルを選択するために必要な情報、たとえばアプリケーション・プログラムのプロダクトナンバー等を含めることができる。

【００３２】インデックス・ファイル取得手段２２２は、インデックス・サーバ３から送信されたインデックス・ファイルを受信する、取得情報デコーダ２２３は、受信したインデックス・ファイルに含まれる暗号を復号化する。本実施の形態では、インデックス・ファイルが暗号化できるため、システムのセキュリティ、特に認証サーバ４のアドレス情報に対するセキュリティを向上できる。

【００３３】ＵＩＤ／ＰＷＤ取得・新ライセンス表示ダイアログ２２４は、認証サーバ４に認証要求を行う際に必要な会員番号等のユーザ識別情報およびパスワードを取得する機能を持つ。また、認証後に付与されることとなる新ライセンスの契約内容を表示する機能を持つ。新ライセンス（契約）文書は、インデックス・ファイルに含めてインデックス・サーバ３から送ることにより、ライセンス更新ごとに新しい内容を表示できる。

【００３４】認証サーバ接続手段２２５は認証サーバ４への認証要求を発する機能を持つ。認証要求には、前記したユーザ識別情報（ＵＩＤ）とパスワード（ＰＷＤ）を含めることができる。認証結果取得手段２２６は、認証サーバ４から送信された認証結果を取得する。認証結果チェック手段２２７は、取得した認証結果をチェックし、認証成功の場合にはライセンス期間を更新してアプリケーション・プログラムの実行を可能にする。アプリケーション実行モジュール２３は、アプリケーション・プログラムを実行する。

【００３５】インデックス・サーバ３には、インデックス選択・送信手段３１とインデックス３２を含む。インデックス選択・送信手段３１はクライアント２からのインデックス・ファイル送信要求を受けて、インデックス３２から適切なインデックス・ファイルを選択し、あるいは適切なインデックス・ファイルを生成して、クライアント２にそのインデックス・ファイルを送信する。なお、インデックス・ファイルはユーザごとあるいはアプリケーション・プログラムごとに予め作成し、インデックス３２に記録することが好ましい。インデックスの選択あるいは生成には、ユーザからの送信要求に含まれるアプリケーション・プログラムの製造番号あるいはユーザ番号を参照できる。

【００３６】認証サーバ４には、認証データ取得手段４１、認証可否判断手段４２、認証結果送信手段４３、会員データベース４４を含む。認証データ取得手段４１は、クライアント２からの認証要求とそれに含まれる認証データ（ＵＩＤおよびＰＷＤ）を受取る。なお、認証データにはＵＩＤおよびＰＷＤ以外のデータが含まれても良い。認証可否判断手段４２は認証データに基づいて認証の可否判断を行う。判断には会員データベース４４を参照する。たとえば会員データベース４４には現在有効な会員をそのＵＩＤとＰＷＤとでデータベース化し、ユーザから送付された、ＵＩＤおよびＰＷＤと一致するか否かを判断して行える。なお、会員データベース４４は認証サーバ４内に有する必要はなく、他のシステムに記録されていてもよい。認証結果送信手段４３は、認証可否判断手段４２で判断した認証結果をクライアント２に送信する。

【００３７】図４は、本実施の形態のライセンス期間の更新方法の一例を示したフローチャートである。ステップ５０のアプリケーション・プログラムの起動から説明を開始する。

【００３８】アプリケーション・プログラムが起動されると、プログラムはライセンス期間と現在日時を取得し（ステップ５１）、現在日時がライセンス期間内であるかを判断する（ステップ５２）。ライセンス期間である場合は、ステップ７２に進んでアプリケーション・プログラムを実行する（ステップ７２）。この場合、ライセンスは有効なので本実施の形態の会員認証は行われず、速やかにアプリケーション・プログラムが実行される。

【００３９】ライセンス期間外である場合、ライセンスは現在無効であるため、会員認証モジュール２２を起動する（ステップ５３）。会員認証モジュールが起動されると、モジュールはインデックス・ファイル取得要求をインデックス・サーバ３に対して発する（ステップ５４）。

【００４０】インデックス・サーバ３は、ユーザからのこの要求を受取り（ステップ５５）、この要求受信を契機としてインデックス・ファイルの選択または生成を行う（ステップ５６）。インデックス・ファイルの選択または生成にはインデックス３２を参照する。インデックス・サーバはこの段階でインデックス・ファイルを暗号化しても良い。暗号化は予め行い、インデックス３２に暗号化インデックス・ファイルを記録しておくことが好ましい。その後、インデックス・サーバ３は暗号化されたインデックス・ファイルをクライアント２に送信する（ステップ５７）。

【００４１】インデックス・ファイルには前記したように認証サーバ４のＵＲＬを含む。このようにユーザはインデックス・サーバ３を参照して認証サーバ４のＵＲＬを取得するので、認証サーバ４のＵＲＬを認証サーバ４によって公開する必要がない。また、クライアント２は本実施の形態の会員認証モジュールを用いる限りインデックス・サーバ３にアクセスすれば、常に最新の認証サーバ４のＵＲＬが取得できる。このため、認証サーバ４のＵＲＬに変更があってもユーザは無関心でよい。また、認証サーバ側ではＵＲＬを変更してもインデックス・サーバ３のインデックス・ファイルを変更するだけでよく、各ユーザへの周知あるいは連絡の必要がない。

【００４２】また、インデックス・ファイルは暗号化されるのでシステムのセキュリティ、特に認証サーバ４のアドレスに対するセキュリティを向上できる。なお、インデックス・ファイルには、認証サーバ４のＵＲＬのほかにライセンス期間やプログラム使用条件等の情報を含めることができる。

【００４３】図５はインデックス・サーバ３が送信するインデックス・ファイルの一例を示す図である。本ファイルはＸＭＬ（extensible markup language）で記述されている。ここでは「url」タグで囲まれた部分に認証サーバ４のＵＲＬが暗号化されて記述されている。また、「information」タグで囲まれた部分には、「frequency」タグで囲まれているライセンス期間、「requirement」タグで囲まれたプログラム使用条件に関するテキストが記述されている。

【００４４】次に、クライアント２が暗号化されたインデックス・ファイルを受信すると（ステップ５８）、この暗号を復号化し平文のインデックス・ファイルを得る（ステップ５９）。図６は復号化した後のインデックス・ファイルの一例を示す。図５と比較して「url」タグで囲まれた部分が意味のある平文になっている。

【００４５】なお、ここではインデックス・ファイルの一部が暗号化・復号化される例を示しているが、インデックス・ファイルの全てが暗号化されても良いことは勿論である。

【００４６】次に、クライアント２は、ＵＩＤ（会員番号）とＰＷＤ（パスワード）を入力する画面を表示する（ステップ６０）。また、この画面にはプログラム使用条件が同時に表示されても良い。

【００４７】図７は、会員番号およびパスワードを入力する画面の一例を示した図である。画面のウィンドウ８０内には、会員番号を入力するフィールド８１とパスワードを入力するフィールド８２を有する。また、サブウインドウ８３にはプログラム使用条件が表示される。この新しいプログラム使用条件にユーザが同意する時には「はい」のボタン８４をクリックし、同意しない時には「いいえ」のボタン８５をクリックする。なお、「いいえ」のボタン８５が押された時にはプログラムは終了する。

【００４８】次に、クライアント２は、たとえば前記フィールド８１，８２に入力されたデータからＵＩＤとＰＷＤを取得し（ステップ６１）、これらデータを認証データとする。なお、ここではユーザ入力により認証データを得る方法を例示したが、たとえばクライアント２のシステム内にユーザ情報を記録し、このユーザ情報から必要なデータを取得して認証データとしても良い。

【００４９】次に、クライアント２は、認証サーバ４に認証の取得要求を発する（ステップ６２）。取得要求には前記ステップで取得したＵＩＤ／ＰＷＤ等の認証データを含める。

【００５０】次に、認証サーバ４がクライアント２からの認証要求を受取り、同時に認証データを受取る（ステップ６３）。認証サーバ４は、クライアントからの要求を契機として、会員データベース４４を検索し（ステップ６４）、認証要求の会員の資格が有効であるかを判断する（ステップ６５）。会員資格が有効である時には、認証成功の「ReturnValue」を生成し（ステップ６６）、会員資格が無効の場合には認証失敗の「ReturnValue」を生成する（ステップ６７）。そしてこの「ReturnValue」を認証結果としてクライアント２に送信する。

【００５１】クライアント２は、「ReturnValue」を受信し（ステップ６９）、「ReturnValue」が認証成功であるかを判断する（ステップ７０）。認証成功の場合、ライセンス期間を新たなライセンス期間に更新し（ステップ７１）、アプリケーション・プログラムを実行する（ステップ７２）。その後処理を終了する（ステップ７３）。認証失敗の場合はライセンス期間を更新することなく、また、アプリケーション・プログラムを実行することなく終了する（ステップ７３）。

【００５２】本実施の形態によれば、ユーザはライセンス期間を経過したプログラムを実行するに際して、プログラム提供者に新たなライセンスの申請、ライセンス期間の更新申請を行う必要がない。本実施の形態では、ライセンス期間の経過を自動的に判断し、認証を自動的に取得できる（ただしユーザＩＤ（会員番号）とパスワードの入力は要求される）。また、本実施の形態によれば、認証サーバ４のアドレスをインデックス・サーバ３から取得するので、認証サーバ４のアドレス変更を容易に行える。また、インデックス・ファイルを認証ごとに取得するので、最新の使用条件等、最新データをユーザに提示できる。さらにインデックス・ファイルを暗号化してシステムのセキュリティを向上できる。

【００５３】以上、本発明者によってなされた発明を発明の実施の形態に基づき具体的に説明したが、本発明は前記実施の形態に限定されるものではなく、その要旨を逸脱しない範囲で種々変更することが可能である。

【００５４】たとえば、前記実施の形態では、プログラム使用の当初からライセンスを与えられている場合を説明したが、当初は試用段階のライセンスが与えられ、その後正式なライセンスが与えられる場合にも適用できる。

【００５５】また、前記実施の形態では、認証サーバ４が単一の場合を説明したが、図８に示すように複数の認証サーバ４－１，４－２を有しても良い。ユーザに異なるプログラム提供者からのプログラムが提供されている時には、提供者ごとに認証サーバを設置し、提供者独自のユーザ（会員）管理を行う場合にも本発明が利用できる。この場合、プログラム提供者が異なっても、図示するように単一のインデックス・サーバを共用することができる。

【００５６】また、図９に示すように、インデックス・サーバと認証サーバを単一のサーバで実現しても構わない。

【００５７】さらに、本発明はライセンス期間を自由に設定できる。そしてライセンス期間の更新が簡便に実現できる本発明は、そのようなライセンス期間を自由に設定したいと望むプログラム提供者やユーザに安全で且つ利便性の高いシステムを提供できるものである。

【００５８】また、前記実施の形態ではインデックス・ファイルの一部または全部が暗号化される例を示したが、インデックス・ファイルは暗号化されなくても良い。

【００５９】

【発明の効果】本願で開示される発明のうち、代表的なものによって得られる効果は、以下の通りである。すなわち、プログラム使用許諾（ライセンス）期間の更新認証事務を効率化することができる。また、ライセンス期間を自動的に更新でき、ユーザおよびプログラム提供者の双方に利便性の高いシステムを提供できる。また、セキュリティおよびフレキシビリティに優れたライセンス更新システムおよび方法を提供できる。

【図面の簡単な説明】

【図１】本発明の一実施の形態であるライセンス期間の更新方法に適用できるシステムの一例を示した概念図である。

【図２】本発明の一実施の形態であるライセンス期間更新の概要について時系列に示した図である。

【図３】クライアント、インデックス・サーバ、認証サーバの構成の一例を示したブロック図である。

【図４】本発明の一実施の形態であるライセンス期間の更新方法の一例を示したフローチャートである。

【図５】インデックス・サーバが送信するインデックス・ファイルの一例を示す図である。

【図６】復号化した後のインデックス・ファイルの一例を示す図である。

【図７】会員番号およびパスワードを入力する画面の一例を示した図である。

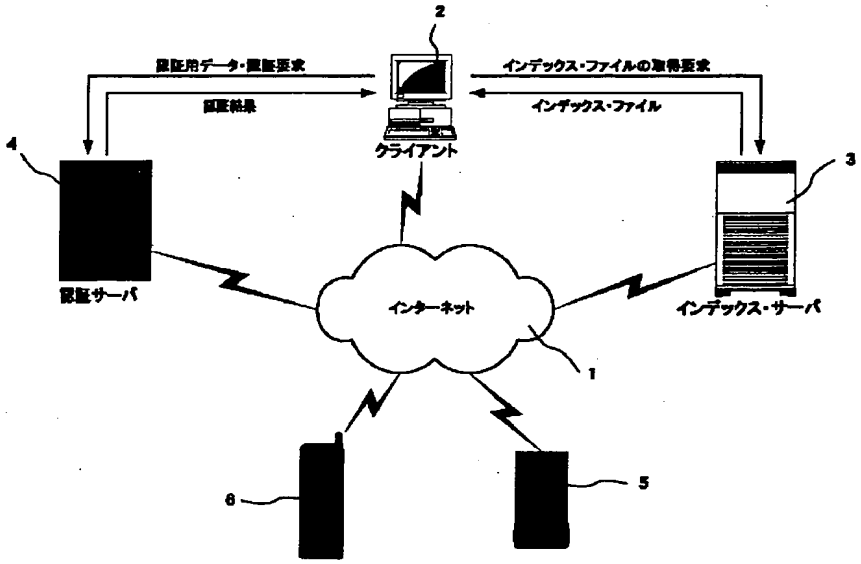
【図８】本発明の他の実施の形態の一例を示したブロック図である。

【図９】本発明の他の実施の形態の他の例を示したブロック図である。

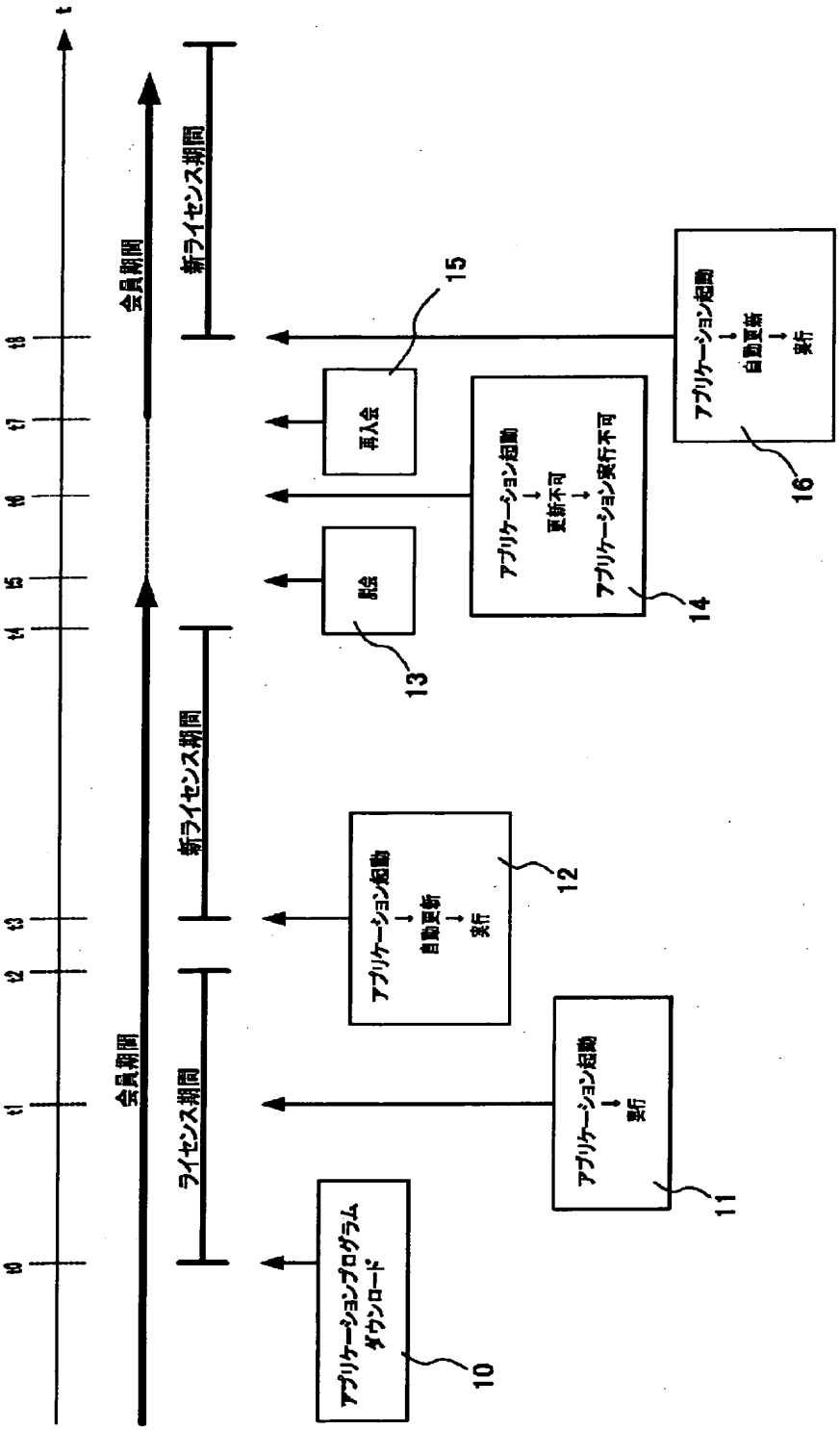
【符号の説明】

１…インターネット、２…クライアント、３…インデックス・サーバ、４…認証サーバ、５…携帯情報端末（ＰＤＡ）、６…携帯電話、２０…アプリケーション・プログラム、２１…ライセンス期間チェックモジュール、２２…会員認証モジュール、２２１…インデックス・サーバ接続手段、２２２…インデックス・ファイル取得手段、２２３…取得情報デコーダ、２２４…ＵＩＤ／ＰＷＤ取得・新ライセンス表示ダイアログ、２２５…認証サーバ接続手段、２２６…認証結果取得手段、２２７…認証結果チェック手段、２３…アプリケーション実行モジュール、２４…時計、３１…インデックス選択・送信手段、３２…インデックス、４１…認証データ取得手段、４２…認証可否判断手段、４３…認証結果送信手段、４４…会員データベース、８０…ウィンドウ、８１，８２…フィールド、８３…サブウインドウ、８４，８５…ボタン、ｔ０～ｔ８…時刻。

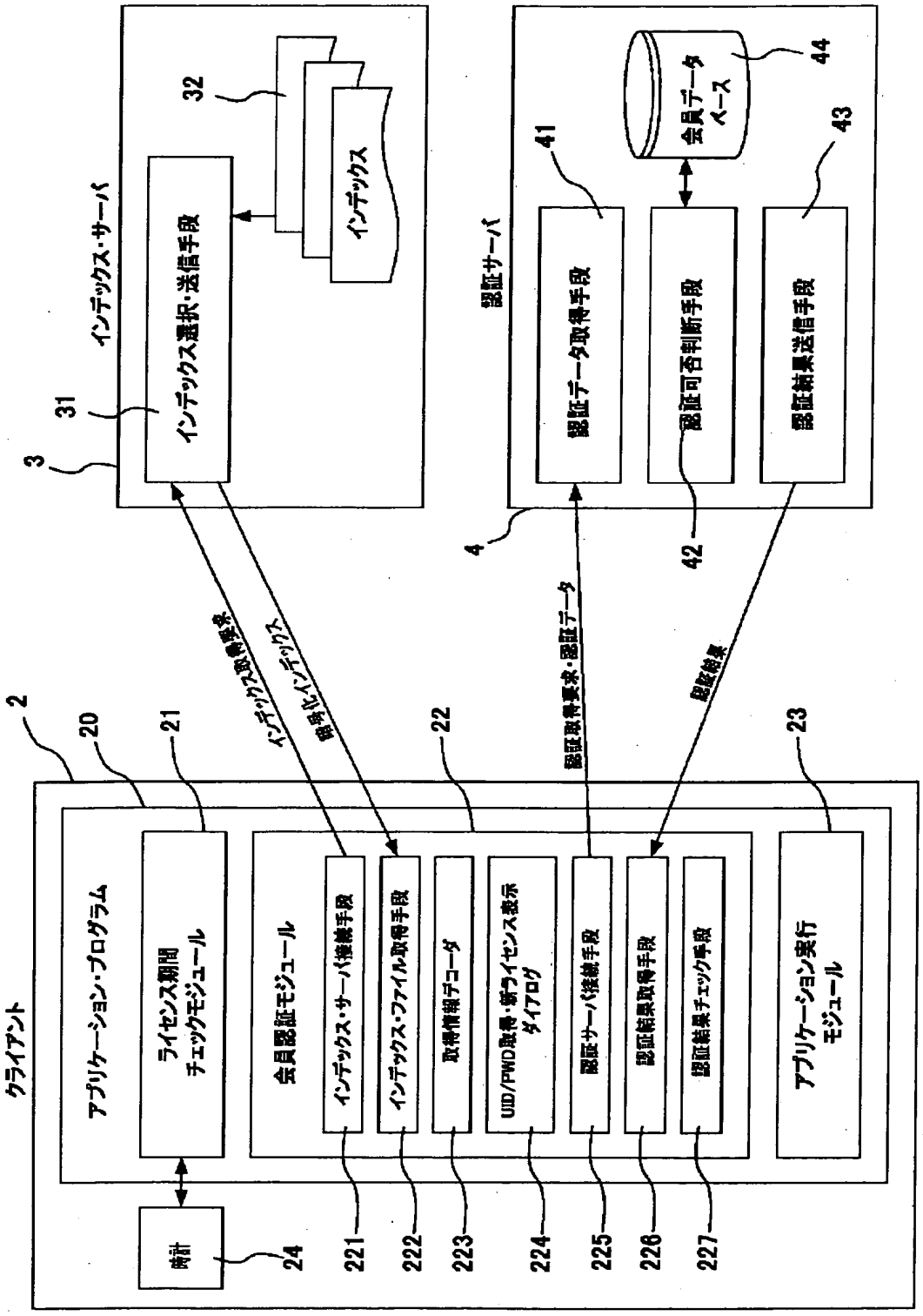
【図１】



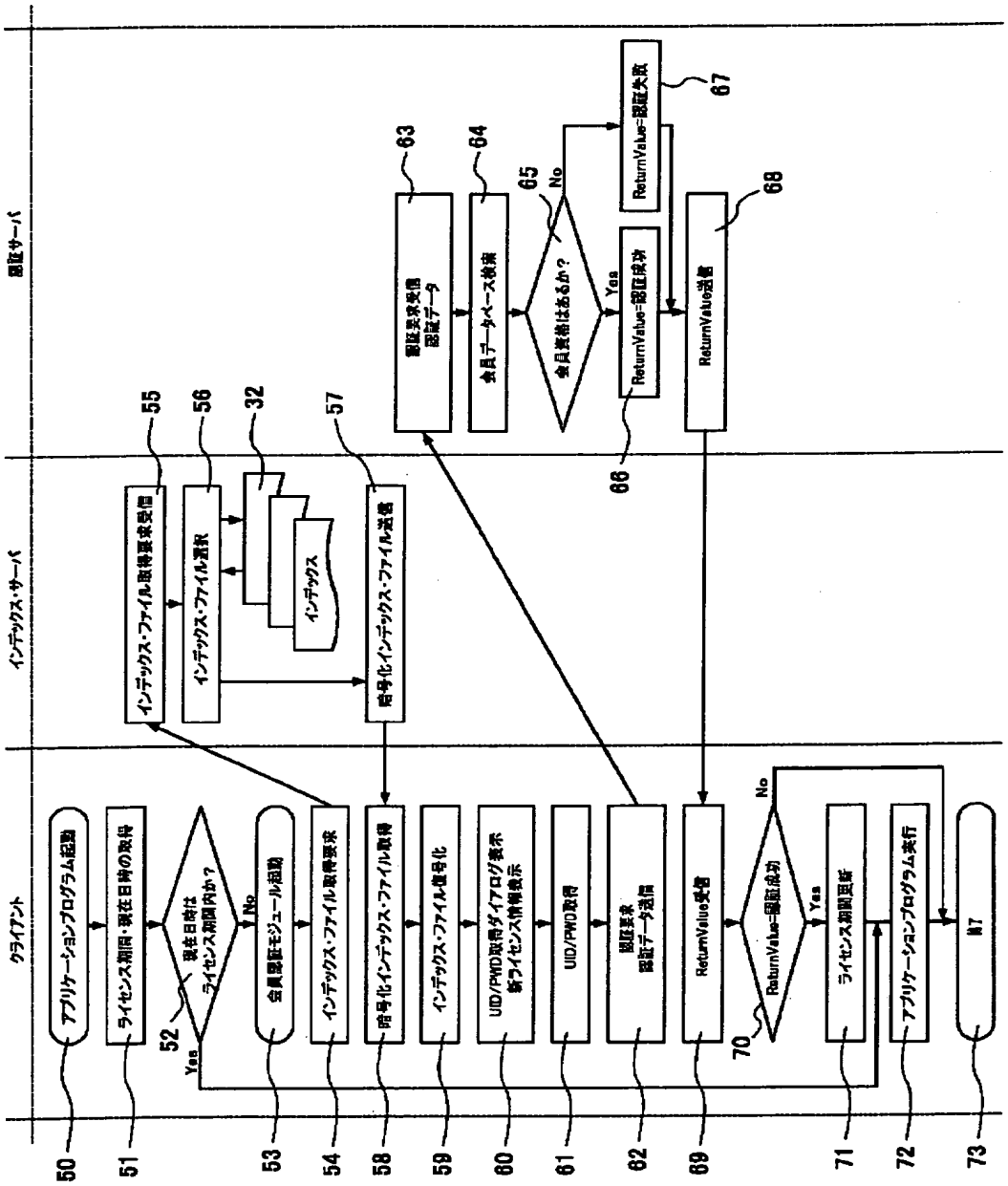
【図２】


t
t0
t1
t2
t3
t4
t5
t6
t7
t8
会員期間
ライセンス期間
新ライセンス期間
会員期間
新ライセンス期間
アプリケーションプログラム
ダウンロード
10
アプリケーション起動
↓
実行
11
アプリケーション起動
↓
自動更新
↓
実行
12
破棄
13
アプリケーション起動
↓
更新不可
↓
アプリケーション実行不可
14
再入会
15
アプリケーション起動
↓
自動更新
↓
実行
16

【図３】


クライアント
2
アプリケーション・プログラム
20
ライセンス期間
チェックモジュール
21
時計
24
会員認証モジュール
22
インデックス・サーバ接続手段
221
インデックス・ファイル取得手段
222
取得情報デコーダ
223
UID/PWD取得・新ライセンス表示
ダイアログ
224
認証サーバ接続手段
225
認証結果取得手段
226
認証結果チェック手段
227
アプリケーション実行
モジュール
23
インデックス取得要求
暗号化インデックス
認証取得要求・認証データ
認証結果
インデックス・サーバ
3
インデックス選択・送信手段
31
インデックス
32
認証サーバ
4
認証データ取得手段
41
認証可否判断手段
42
認証結果送信手段
43
会員データベース
44

【図４】


クライアント
インデックス・サーバ
認証サーバ
アプリケーションプログラム起動
ライセンス期間・現在日時の取得
現在日時はライセンス期間内か？
Yes
No
会員認証モジュール起動
インデックス・ファイル取得要求
暗号化インデックス・ファイル取得
インデックス・ファイル復号化
UID/PWD取得ダイアログ表示
新ライセンス情報表示
UID/PWD取得
認証要求
認証データ送信
ReturnValue受信
ReturnValue=認証成功
ライセンス期間更新
アプリケーションプログラム実行
終了
インデックス・ファイル取得要求受信
インデックス・ファイル選択
インデックス
暗号化インデックス・ファイル送信
認証要求受信
認証データ
会員データベース検索
会員登録はあるか？
ReturnValue=認証失敗
ReturnValue送信
50
51
52
53
54
58
59
60
61
62
69
70
71
72
73
55
56
32
57
63
64
65
66
67
68

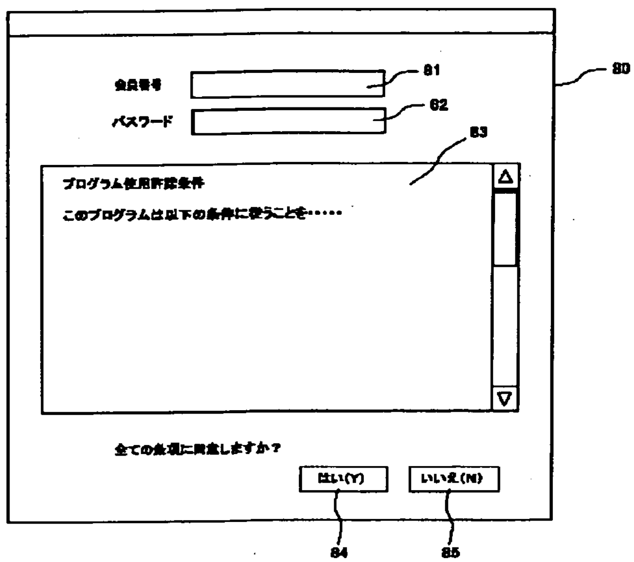
【図5】

```
<?xml version='1.0' encording='SHIFT_JIS' ?>
<pkm-taxonnomy version="1.0" local save="no">
<description>user authentication server</description>
<site>
<url>aabbbccdseiiiissel#$$$&&&・・・・・・・・・・・・・・・・・・・・・・
・・・・・・・・・・・・・・・・・・・・・・・・・aashhhjjjdkkifir</url>
<information>
<frequency>365</frequency>
<requirement>プログラム使用許諾条件
このプログラムは以下の条件に従うことを・・・・・
</requirement>
</information>
</site>
</pkm-taxonnomy>
```

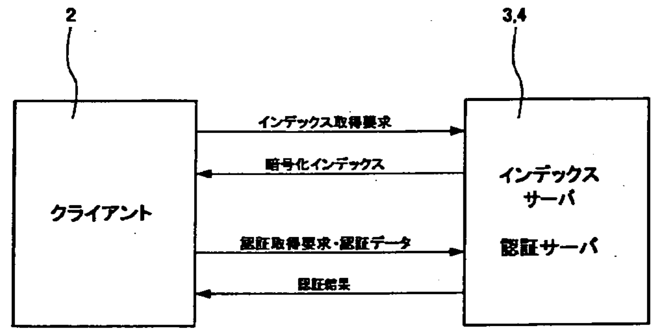
【図6】

```
<?xml version='1.0' encording='SHIFT_JIS' ?>
<pkm-taxonnomy version="1.0" local save="no">
<description>user authentication server</description>
<site>
<url>https://www.abcd.com/cgi-bin/abc_club/index.cgi?html=index.html</url>
<information>
<frequency>365</frequency>
<requirement>プログラム使用許諾条件
このプログラムは以下の条件に従うことを・・・・・
</requirement>
</information>
</site>
</pkm-taxonnomy>
```

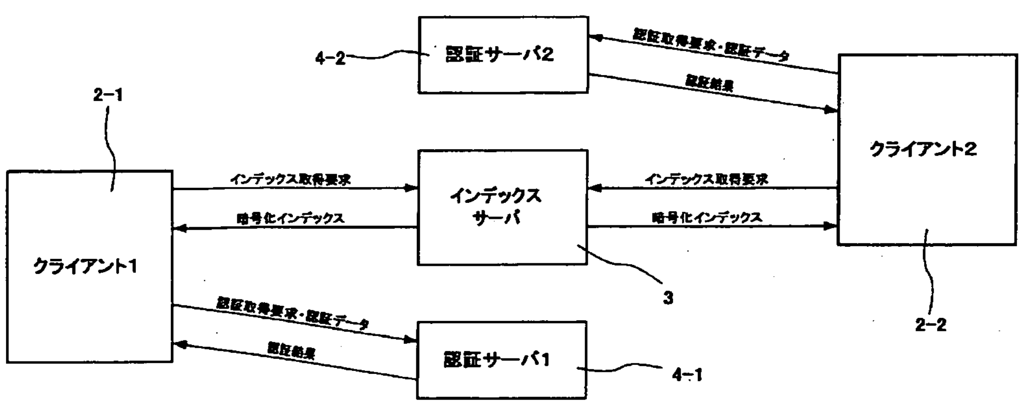
【図7】



【図9】



【図8】



フロントページの続き

(72)発明者　川口　佳文
神奈川県大和市下鶴間1623番地14　日本アイ・ビー・エム株式会社　大和事業所内

(72)発明者　中垣　勝博
東京都港区六本木三丁目２番12号　日本アイ・ビー・エム株式会社内

Ｆターム(参考)　5B076 FA00 FB01 FB11